F. Christopher Austin (NV Bar No. 6559)
Email: caustin@weidemiller.com
WEIDE & MILLER, LTD.
10655 Park Run Drive
Suite 100
Las Vegas, NV 89144
Telephone: (702) 382-4804
Facsimile: (702) 382-4805

Nathaniel L. Dilger (CA Bar No. 196203)
Email: ndilger@onellp.com
Peter R. Afrasiabi (CA Bar No. 193336)
Email: pafrasiabi@onellp.com
ONE LLP
23 Corporate Plaza
Suite 150-105
Newport Beach, CA 92660
Telephone: (949) 502-2870
Facsimile: (949) 258-5081

William J. O'Brien (CA Bar No. 99526)
Email: wobrien@onellp.com
ONE LLP
9301 Wilshire Blvd
Penthouse Suite
Beverly Hills, CA 90210
Telephone: (310) 866-5157
Facsimile: (949) 943-2085

Attorneys for Plaintiff,
FaceTec, Inc.

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

FACETEC, INC., a Delaware corporation, Plaintiff, v. iPROOV LTD, a United Kingdom limited liability company, Defendant.	Case No. **COMPLAINT FOR:** **(1) PATENT INFRINGEMENT;** **(2) BREACH OF CONTRACT** **(3) INTENTIONAL INTERFERENCE WITH CONTRACTUAL RELATIONS** **JURY DEMAND**

COMPLAINT

Plaintiff FaceTec, Inc. ("FaceTec" or "Plaintiff") hereby complains and alleges against Defendant iProov Ltd. ("iProov" or "Defendant") as follows:

PARTIES

1. Plaintiff FaceTec is a Delaware limited liability company with its principal offices located at 1925 Village Center Cir., Ste 150, Las Vegas, NV 89134.

2. FaceTec is informed and believes that Defendant iProov is a United Kingdom limited liability company with a regular and established place of business at 10 York Rd, London SE1 7ND, United Kingdom.

NATURE OF THE ACTION

3. This is an action for patent infringement arising under the patent laws of the United States 35 U.S.C. §§ 1 *et seq.*, including 35 U.S.C. § 271, and the Court's supplemental jurisdiction pursuant to 28 U.S. Code § 1367.

4. FaceTec is informed and believes that Defendant has infringed and continues to infringe, contribute to the infringement of, and/or actively induce others to infringe Plaintiff's U.S. Patent No. 10,776,471 B2 (the "'471 patent" or the "patent-in-suit"). Ex. A.

5. In addition, FaceTec is informed and believes that Defendant has breached and continues to breach its contractual obligations to FaceTec.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this patent infringement action pursuant to 28 U.S.C. §§ 1331 and 1338 and supplemental jurisdiction over FaceTec's claim for breach of contract pursuant to 28 U.S. Code § 1367.

7. This Court has personal jurisdiction over iProov because iProov does and has done substantial business in this judicial District, including: (i) committing acts of patent infringement and/or contributing to or inducing acts of patent infringement by others in this judicial District and elsewhere in this State; (ii) regularly conducting business in this State and judicial District; (iii) directing advertising to or soliciting business from persons residing in this State and judicial

District; and (iv) engaging in other persistent courses of conduct, and/or deriving substantial revenue from products and/or services provided to persons in this District and State.

8. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391 and 1400(b). iProov has transacted business in this district and has committed acts of patent infringement in this District. And as a foreign entity, iProov may be sued in this District because "a defendant not resident in the United States may be sued in any judicial district." 28 U.S.C. § 1391(c)(3); *see also Brunette Machine Works, Ltd. v. Kockum Industries, Inc.*, 406 U.S. 706 (1972).

FACTUAL BACKGROUND

9. FaceTec is a leader in biometric liveness detection. Simply explained, this technology allows face image data collected to verify the physical presence of a live human with high confidence, i.e., the face image data of a person is used to verify the presence of that person to create a new digital account or provide authorized access to an existing account. The liveness detection technology provided by FaceTec utilizes the image data of the user's face to prove the user is physically present. Once the user's liveness is proven to a high confidence and the collected face data also matches the expected face data with high confidence, the user may then be allowed access to a protected computer, smartphone, bank account, etc.

A. FaceTec's biometric liveness technology.

10. Liveness detection seeks to ensure that a live human is present and in front on the camera at the time biometric face data is collected. For example, liveness detection would detect if – rather than an actual living person being imaged at the time of data collection– an attempt to spoof the liveness detection software is being perpetrated. For example, a fraudster might present an artifact such as a 2-dimensional (2D) photo of a face, or a video of a face that was prerecorded, or might attempt to bypass the camera sensor entirely and inject a video stream directly into the device's hardware, operating system, or web browser software.

11. Liveness detection alone offers significant security benefits but is often paired with biometric face matching to enable remote user authentication or user identity verification. Remote user identity verification generally includes the following steps[1]:

- Capture one or more photos or video frames of the user's face.
- Perform a liveness check to determine if the source of the face data is a live and physically present human, or if the captured data is from a pre-collected artifact.
- Capture one or more images of a Photo ID document.
- Extract text data from Photo ID and any barcode or NFC chip present with the document.
- Compare the liveness-proven image data to the face image data on the Photo ID or NFC chip, or in a trusted identity issuer's database.

12. FaceTec's technology for liveness detection inspects and analyzes numerous different aspects of the face images collected by the camera sensor. One very important aspect analyzed is "perspective distortion," which, when present, verifies to a high level of confidence that the source of the face data was 3D. The FaceTec software performs this function by collecting one or more face images at a first distance from the camera, collecting one or more face images at a second distance from the camera, and then comparing the images to confirm the presence of perspective distortion and hence exhibit photographic evidence of 3-dimensionality.

13. The following two images simulate the expected changes in the appearance of a 3D face when the capture distance is changed. As can be seen below, perspective distortion causes the user's nose to swell in proportion to the rest of the face, as well as other subtle but detectable distortions in the face shown in the second image as compared to the face of the first image. FaceTec's software measures the perspective distortion between at least two images taken at different distances between the subject and the camera.

[1] The order of operation may vary.

First Image Second Image

14. By measuring/confirming various indicia such as 3D face depth, skin texture, eye reflections, etc., the FaceTec software is able to confirm a user's liveness with exceptionally high confidence.

15. Other organizations have attempted to use 2D images to detect the liveness of the user using either a single photo, or a series of photos taken at the same distance. 2D liveness, however, simply does not have the necessary accuracy to detect today's sophisticated threats. Additionally, 2-dimensional face matching is more vulnerable to impersonation attacks because many people have high resolution photos posted online that can be used as spoof artifact source material.

16. Alternatively, hardware-based 3D systems have also been used, including Apple's "Face ID," which allows a user to unlock their iPhone simply by looking at the device. Apple's Face ID system, however, requires specialized infrared cameras that are built into the phone screen to confirm 3D depth as part of its liveness analysis. But this need for special hardware means this

technology cannot be utilized by the vast majority of current smart device owners around the world, whose devices do not include built-in infrared cameras. In contrast, FaceTec's 3D liveness detection software can be implemented on virtually any device having a 2D camera, which includes almost all modern laptop computers, smartphones, and desktop computers. Overall, FaceTec's software solution can be used on an estimated 10 billion Android & iOS devices, smartphones, and computers with webcams.

17. Currently, FaceTec's technology provides approximately 500 million liveness checks annually on six continents and for all combinations of user age, gender, ethnicity and device type.

B. FaceTec's patent portfolio.

18. FaceTec has sought protection for its technological innovations, which has resulted in the issuance of the '471 patent-in-suit as well as other related patents.

19. The '471 patent issued on June 10, 2014 and is titled "Facial recognition authentication system including path parameters." FaceTec is the owner of the '471 patent. Ex. A.

20. Additional patents issued to FaceTec include the following:

- 11,157,606: "Facial recognition authentication system including path parameters"
- 10,915,618: "Method to add remotely collected biometric images / templates to a database record of personal information"
- 10,803,160: "Method to verify and identify blockchain with user question data"
- 10,698,995: "Method to verify identity using a previously collected biometric image/data"
- 10,614,204: "Facial recognition authentication system including path parameters"
- 10,262,126: "Facial recognition authentication system including path parameters"

- 9,953,149: "Facial recognition authentication system including path parameters"
- D813,264: "Display screen or portion thereof with graphical user interface"

21. In addition, FaceTec owns nearly a dozen pending U.S. and foreign patent applications on its technology.

C. FaceTec's "Spoof Bounty Program"

22. FaceTec's intense development of its liveness detection software included years of testing its software against tens of millions of digital and physical spoof attempts, including:

- 2D paper photos & digital images
- High resolution videos
- Paper masks with eye & mouth cutouts
- "Hollywood" quality masks, wax figures & lifelike dolls
- Photos or video frames animated into avatars
- Video projections on 3D heads
- Device Emulators & Virtual Camera programs
- Hardware Video Injection converters & adapters

23. To further enhance the security of its product, in October 2019, FaceTec publicly implemented a "Spoof Bounty Program," whereby, in exchange for agreeing to FaceTec's terms and conditions, any interested party would be permitted access to FaceTec's Bounty Program to try to spoof or bypass the FaceTec software. If the participant successfully spoofed or bypassed the system, they were to notify FaceTec of the details of the successful attack so that FaceTec could use this information to mitigate that threat vector and thereby make its software more secure.

24. FaceTec has, since October 2019, offered participants a bounty (monetary reward) for any successful attacks to encourage people to participate in the program. The amount of this bounty is based on the type of attack successfully used. The Bounty Program currently includes the following attack vectors and bounty payout amounts:

How to Participate in the Bounty Program

Successfully Spoof or Bypass FaceTec's Liveness Detection with a method that qualifies as Level 1, 2, 3, 4 or 5 on the Liveness.com (http://www.liveness.com) Threat Vector Scale, reproduce it, and be paid a bounty as follows:

Threat	Description	Example	Bounty
Level 1	Hi-res paper & digital photos, hi-def videos exhibiting challenge/response and human-worn paper masks.		$15,000
Level 2	Commercially available lifelike dolls, and resin, latex & silicone 3D masks up to USD$300 in price.		$15,000
Level 3	Custom-made ultra-realistic 3D masks, sculptures, wax heads, etc. up to USD$3,000 in creation costs.		$20,000
Level 4	Successfully decrypt & edit the contents of a 3D FaceScan to contain synthetic data not collected from the session, have the Server SDK process it and respond with Liveness Success.	3D FaceScan Tampering (https://dev.facetec.com/security-best-practices#facemap-tampering)	$30,000
Level 5	Successfully take over the camera feed & inject previously captured frames that result in the Server SDK responding with Liveness Success.	ManyCam (https://manycam.com/) Vcam (https://www.e2esoft.com/vcam/) vlc2Cam (https://vlc2vcam.com/) FakeWebcam (https://www.fakewebcam.com/)	$20,000

25. Through the Spoof Bounty Program, FaceTec has uncovered two previously unknown vulnerabilities in FaceTec's Liveness software's security layers. This information has allowed FaceTec to patch the newly discovered vulnerabilities and thereby elevate the anti-spoofing capabilities and overall security even further. Today, all known threat vectors are mitigated by the FaceTec algorithms, which utilize neural networks along with other artificial intelligence and machine learning techniques.

26. Given that participants were granted special access to the FaceTec Spoof Bounty Program software, participation in the Bounty Program understandably included several significant restrictions. Without exception, participants are required to agree to use any information learned during participation in FaceTec's Spoof Bounty Program solely for that program. Participants cannot reverse engineer the FaceTec software and use that information in

any other liveness detection product or service, and participants are required to hold all information learned through the Spoof Bounty Program strictly confidential:

> Any information you receive or collect about FaceTec, its customers, technology, software, applications, performance, security methods and other related information through the Spoof Bounty Program ("Confidential Information") must be kept confidential and only used in connection with the Spoof Bounty Program. You may not use, disclose or distribute any such Confidential Information, including, but not limited to, any information regarding your Submissions and information you obtain when researching the FaceTec products and services, without FaceTec's prior written consent. You may not use any of the information, concepts, computer code, security techniques, sequencing or strategies that you may learn from attempting to reverse engineer FaceTec's technology during your participation in the Spoof Bounty Program or using the bounty.facetec.com page in any other Liveness Detection product or service offered by any other company. If you do use information that you learn from interacting with FaceTec's technology in any other Liveness Detection Product or Service, you will be held liable for intellectual property theft and will be prosecuted to the fullest extent of the applicable laws.

27. FaceTec maintained detailed records of all participants in its Spoof Bounty Program, as well as testers of its Demo Applications and Developer accounts. And these records show that – in addition to many legitimate participants – certain iProov executives/employees participated extensively in the FaceTec Spoof Bounty Program and the FaceTec Demo Applications. Indeed, it is estimated that iProov executives and employees spent over 80 hours conducting extensive probing attacks of the FaceTec software. And as explained further below, iProov thereafter improperly used the information it learned through these attacks in direct contravention of its contractual obligations to FaceTec.

/ / /

/ / /

D. Defendant iProov and the "Liveness Assurance" product

28. Defendant iProov is well aware of both FaceTec and its patented technology. iProov makes software called "Liveness Assurance, which competes with FaceTec's software. This offering – with aspects copied from FaceTec – performs biometric liveness detection. According to iProov's web site:

> iProov's Liveness Assurance technology attempts to verify that a face presented to a mobile device is from a live human being. It identifies if a photograph or video or mask is being used to attempt to spoof the biometric security system as part of a presentation attack. It confirms that a user is:
>
> 1. A real person – this person is a human being and not a photo, a mask, or other presentation attack.

https://www.iproov.com/iproov-system/technology/liveness-assurance.

29. As alleged herein, iProov's Liveness Assurance product infringes at least FaceTec's '047 patent. In addition, the Liveness Assurance product also improperly incorporates aspects of FaceTec's technology that iProov learned through its participation in the Spoof Bounty Program and unauthorized use of the FaceTec software outside of the Spoof Bounty Program.

30. As noted above, numerous iProov executives and employees conducted extensive probing attacks of the FaceTec software. But rather than comply with the requirements of the Spoof Bounty Program, which required confidentiality for any of the information learned through its participation, iProov instead directly violated the requirements imposed on all participants in the Spoof Bounty Program. In particular, iProov improperly reverse engineered FaceTec's software and used the information gleaned therefrom to create iProov's Liveness Assurance software.

31. In addition, one iProov employee (Joseph Palmer) spent an estimated 80 hours attempting Level 5 camera bypass attacks in June-July of 2020, even though there was no financial bounty offered to incentivize that type of attack during that time frame. That iProov employee continued to participate in the bounty until at least January 2021, gleaning more and more information about how the FaceTec software worked. Shortly thereafter in 2021, iProov released

its "Liveness Assurance" software and included in it a security technique that FaceTec refers to as "Camera Cycling," as well as a user interface which required users to provide images of their face from at least two different distances.

32. On information and belief, iProov improperly used the additional information gleaned during its participation in the Spoof Bounty Program to reverse engineer portions of the FaceTec software and added aspects of FaceTec software to its own Liveness Assurance software.

33. In addition, iProov disclosed to at least one third party, a FaceTec partner, details about information iProov learned from its participation in the Spoof Bounty Program, which it was required to keep confidential. This was done in direct violation of the contractual obligations established to FaceTec by all Bounty Program participants when they accepted the FaceTec Bounty Program terms and conditions prior to gaining access to the FaceTec Bounty Program software.

34. After uncovering evidence of the reverse engineering, FaceTec contacted iProov in writing on or about September 9, 2021, and demanded that iProov immediately cease and desist its improper use of any and all technology learned by iProov during its exhaustive reverse engineering as well as any technology that falls under the scope of FaceTec's patents.

35. While iProov responded to this letter shortly thereafter, it refused FaceTec's demand to cease and desist and refused to address the unauthorized use of information it learned regarding FaceTec's Liveness detection software. Faced with this refusal, FaceTec had no choice but to pursue this lawsuit.

FIRST CLAIM FOR RELIEF

(Infringement of the '471 Patent – 35 U.S.C. §§ 271 *et seq*.)

36. Plaintiff realleges and incorporates by reference the foregoing paragraphs, as though fully set forth herein.

37. Defendant iProov has had actual knowledge of the '471 patent. For example, in September of 2021 FaceTec contacted iProov in writing, specifically notifying iProov that the Liveness Assurance product infringed at least Claim 10 of the '471 patent. Despite having full knowledge of the '471 patent and its infringement of that patent, Defendant has directly infringed

and continues to directly infringe one or more claims of the ’471 patent by developing, making, using, offering to sell, selling and/or importing, in this District, elsewhere in the United States, and internationally, iProov’s Liveness Assurance product (the “Accused Product”). For example, as shown in the chart attached as **Exhibit B**, users of the Accused Product (whether iProov customers or iProov itself) infringe at least claim 10 of the ’471 patent.

38. iProov also has induced the direct infringement of its customers and continues to induce infringement one or more claims of the ’471 patent by developing, making, using, offering to sell, selling and/or importing, in this District and elsewhere in the United States, the Accused Product. Among other things, iProov has – with full knowledge of the ’471 patent and its applicability to the Accused Product – specifically designed the Accused Product in a manner that infringes the ’471 patent and has also specifically instructs users of the Accused Product – via on screen visual guidance and/or online instructional materials – to use the Accused Product in a manner that infringes one or more claims of the ’471 patent, including at least claim 10.

39. Moreover, iProov has contributed to the infringement of and continues to contributorily infringe one or more claims of the ’471 patent by developing, making, using, offering to sell, and selling the Accused Product in this District, elsewhere in the United States, and internationally. In particular, iProov developed, made, used, offered to sell, sold and/or imported the Accused Product with full knowledge of the ’471 patent and its applicability to the Accused Product. In addition, the Accused Product is a non-staple article of commerce that has no substantial use other than in a manner that infringes one or more claims of the ’471 patent, including at least claim 10.

40. iProov’s actions constitute direct infringement, contributory infringement, and/or active inducement of infringement of one or more claims of the ’471 patent in violation of 35 U.S.C. § 271.

41. FaceTec has sustained damages and will continue to sustain damages as a result of Defendant’s aforesaid acts of infringement.

42. FaceTec is entitled to recover damages sustained as a result of iProov’s wrongful acts in an amount to be proven at trial.

43. iProov's infringement of FaceTec's rights under the '471 patent will continue to damage Plaintiff's business, causing irreparable harm, for which there is no adequate remedy at law, unless it is enjoined by this Court.

44. In addition, iProov has infringed the '471 patent – directly, contributorily, and by inducement – with full knowledge of the '471 patent and despite having full knowledge that its actions constituted infringement of that patent. For at least this reason, iProov has willfully infringed the '471 patent, entitling FaceTec to increased damages under 35 U.S.C. § 284 and to attorney fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

SECOND CLAIM FOR RELIEF

(Breach of Contract)

45. FaceTec realleges and incorporates by reference the foregoing paragraphs, as though fully set forth herein.

46. Participation in FaceTec's Spoof Bounty Program required that all participants accept the terms and conditions of that program. Among other things, these terms and conditions required that participants use information learned during participation in FaceTec's Spoof Bounty Program solely for that program. The terms and conditions clearly state that the participants must agree not to use any information that they learn in any other liveness detection product or service, and would hold all information learned through the Spoof Bounty Program in strict confidentiality:

> Any information you receive or collect about FaceTec, its customers, technology, software, applications, performance, security methods and other related information through the Spoof Bounty Program ("Confidential Information") must be kept confidential and only used in connection with the Spoof Bounty Program. You may not use, disclose or distribute any such Confidential Information, including, but not limited to, any information regarding your Submissions and information you obtain when researching the FaceTec products and services, without FaceTec's prior written consent. You may not use any of the information, concepts, computer code, security techniques, sequencing or strategies that you

may learn from attempting to reverse engineer FaceTec's technology during your participation in the Spoof Bounty Program or using the bounty.facetec.com page in any other Liveness Detection product or service offered by any other company. If you do use information that you learn from interacting with FaceTec's technology in any other Liveness Detection Product or Service, you will be held liable for intellectual property theft and will be prosecuted to the fullest extent of the applicable laws.

47. By participating in FaceTec's Spoof Bounty program, iProov personnel accepted all terms and conditions of that program, including the terms and conditions set forth above, and formed thereby a valid and enforceable contract with FaceTec.

48. Plaintiff FaceTec either performed any necessary contractual obligations or was excused from performance of those obligations. For example, FaceTec provided all participants, including the participating iProov employees access to the FaceTec software so that they could attempt to uncover any vulnerabilities in that software and recover a bounty thereby.

49. iProov, however, breached the terms of its contract with FaceTec. These breaches included that:

- iProov did not keep confidential the information that it received or collected about FaceTec, its technology, software, applications, performance, security methods and other related information through the Spoof Bounty Program ("Confidential Information"), and in fact disclosed some information about their experience with the Bounty Program to at least one FaceTec partner in an improper attempt to gain an unfair competitive advantage against FaceTec;
- iProov used the Confidential Information for purposes outside of the Spoof Bounty Program;
- iProov used, disclosed and/or distributed Confidential Information outside of the Spoof Bounty Program and without FaceTec's prior written consent;

- iProov used the information, concepts, computer code, security techniques, sequencing or strategies that it learned from the Spoof Bounty Program to attempt to reverse engineer FaceTec's technology; and
- iProov used the information, concepts, computer code, security techniques, sequencing or strategies that it learned from the Spoof Bounty Program to incorporate into its own liveness detection product -- Liveness Assurance.

50. As a result of these actions, FaceTec suffered damage thereby, including that iProov gained an unfair competitive advantage against FaceTec.

THIRD CLAIM FOR RELIEF

(Intentional Interference with Contractual Relations)

51. As alleged herein, iProov personnel chose to participate in the FaceTec Spoof Bounty Program, thereby creating a valid and existing contractual relationship with FaceTec.

52. iProov was aware of the contractual relationship between FaceTec and the iProov personnel who participated in the FaceTec Spoof Bounty Program and the contractual obligations owed thereby to FaceTec. Despite this knowledge, iProov engaged in intentional acts that were intended or designed to disrupt this contractual relationship, including encouraging or directing the personnel to breach their contractual obligations to FaceTec.

53. Because of these intentional acts by iProov, one of more of the iProov employees that chose to participate in the FaceTec spoof bounty program in fact did actually breach their contractual obligations to FaceTec, including by misusing information gleaned from their participation in violation of the explicit terms of that program.

54. As a result of these breaches, FaceTec suffered damages thereby, including being put at a competitive disadvantage as a result of iProov's conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff FaceTec asks this Court to enter judgment in their favor and against Defendant iProov and grant the following relief:

A. An adjudication that iProov has willfully infringed and continues to willfully infringe the patent-in-suit.

B. An adjudication that iProov has breached its contractual obligation to FaceTec.

C. Orders of this Court temporarily, preliminarily, and permanently enjoining iProov, its agents, servants, and any and all parties acting in concert with them, from directly or indirectly infringing in any manner any of the claims of patent-in-suit and from further breaching iProov's contractual obligations to FaceTec;

D. An award of damages – in an amount to be proven at trial – adequate to compensate FaceTec for iProov's infringement of the patent-in-suit and for iProov's breach of contract;

E. A finding that this is an exceptional case and an award of FaceTec's costs and attorney fees;

F. A trebling of the damage award to FaceTec;

G. An assessment and award of pre- and post-judgment interest on all damages awarded; and

H. Any further relief that this Court deems just and proper.

Dated: December 28, 2021

WEIDE & MILLER, LTD.
By: */s/ F. Christopher Austin*
F. Christopher Austin

ONE LLP
Nathaniel L. Dilger
Peter R. Afrasiabi
William J. O'Brien

Attorneys for Plaintiff,
FaceTec, Inc.

DEMAND FOR JURY TRIAL

Plaintiff FaceTec hereby demands a trial by jury as to all claims and all issues properly triable thereby.

Dated: December 28, 2021

WEIDE & MILLER, LTD.
By: */s/ F. Christopher Austin*
F. Christopher Austin

ONE LLP
Nathaniel L. Dilger
Peter Afrasiabi
William J. O'Brien

Attorneys for Plaintiff,
FaceTec, Inc.